

Passwortsicherheit

Stand: 16.03.2016

Jahrgangsstufen	Lernbereich 1: Modul 1.8
Fach/Fächer	Informationstechnologie
Übergreifende Bildungs- und Erziehungsziele	Technische Bildung Ökonomische Verbraucherbildung
Zeitraumen	2 Doppelstunden
Benötigtes Material	Software zum Gestalten und Präsentieren, ggf. Smartphone

Kompetenzerwartungen

Die Schülerinnen und Schüler

- nutzen ihre Kenntnisse zu Risiken sowie Sicherheitsregeln und -maßnahmen im Umgang mit Daten, um diese gezielt vor Verlust und Missbrauch zu schützen.

Aufgabe

Passwörter sind Zeichenfolgen mithilfe derer sich Personen in der Computerwelt ausweisen (identifizieren) oder bestimmte Berechtigungen nachweisen können. Dies funktioniert nur so lange das Passwort geheim bleibt.

Der richtige Umgang mit Passwörtern ist ein sehr wichtiges und gleichzeitig auch vielschichtiges Thema. Um die vielen Aspekte rund um das Thema Passwortsicherheit zusammenzutragen, bearbeitet ihr in Gruppen die folgenden Themen:

- Gruppe 1: Unsichere Passwörter: wie sie gestohlen und gehackt werden
- Gruppe 2: Sichere Passwörter: wie man sie sich ausdenkt und merkt
- Gruppe 3: Passwort-Manager: wie man viele Passwörter im Griff hat

Nach der gemeinsamen Arbeit präsentiert jede Gruppe ihre Ergebnisse.

Hinweise für die Gruppe 1

Auf folgende Aspekte könntet ihr in eure Präsentation eingehen:

- Was sind unsichere Passwörter und warum sind sie unsicher?
- Der Wörterbuchangriff: ein Beispiel für das Hacken unsicherer Passwörter
- Was kann der Angreifer mit geklauten Zugangsdaten alles anstellen?
- Liste mit Verboten: Was darf man im Hinblick auf Passwörter niemals tun?

Mögliche Anlaufstellen für eure Recherchen

- <http://www.sicherespasswort.com>, eingesehen am 22.11.2015



- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, eingesehen am 22.11.2015
- <https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html>, eingesehen am 22.11.2015
- <http://www.faz.net/aktuell/feuilleton/medien/liste-der-schlechtesten-passwoerter-2014-13382590.html>, eingesehen am 22.11.2015
- <https://de.wikipedia.org/wiki/W%C3%B6rterbuchangriff>, eingesehen am 22.11.2015
- <http://www.ndr.de/nachrichten/netzwelt/Identitaetsdiebstahl-im-Netz-was-tun-hilfe,identitaetsdiebstahl102.html>, eingesehen am 22.11.2015

Tipps für eure Präsentation

- Gestaltet einen kleinen Flyer, der die wichtigsten Aspekte eures Themas stichpunktartig und übersichtlich festhält.
- In einem kleinen selbstgemachten Smartphone-Video zu Beginn eurer Präsentation könntet ihr eine typische Situation zeigen, in der ein Benutzer z. B. einen Identitätsdiebstahl bemerkt, weil er ein unsicheres Passwort verwendet hat.

Hinweise für die Gruppe 2

Auf folgende Aspekte könntet ihr in eurer Präsentation eingehen:

- Wie sieht ein sicheres Passwort aus und warum ist es sicher?
- Wie kann man selbst ein sicheres Passwort erstellen, welches gut zu merken ist?
- Was sind Passwort-Generatoren?
- Liste mit Geboten: Was ist zu tun, damit sichere Passwörter entstehen und diese nicht gehackt werden?

Mögliche Anlaufstellen für eure Recherchen

- <http://www.sicherespasswort.com>, eingesehen am 22.11.2015
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, eingesehen am 22.11.2015
- <https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html>, eingesehen am 22.11.2015
- <http://www.stern.de/tv/10-tipps-so-erstellen-sie-sichere-passwoerter-3136120.html>, eingesehen am 22.11.2015

Tipps für eure Präsentation

- Gestaltet einen kleinen Flyer, der die wichtigsten Aspekte eures Themas stichpunktartig und übersichtlich festhält.
- Zeigt ein anschauliches Beispiel für ein selbst erstelltes Passwort – z. B. aus den Anfangsbuchstaben eines Satzes, angereichert mit Ziffern und Sonderzeichen.
- Zeigt einen Online-Passwort-Generator.

Hinweise für die Gruppe 3

Auf folgende Aspekte könntet ihr in eure Präsentation eingehen:

- Was sind Passwort-Manager und welche gibt es?
- Wie funktionieren Passwort-Manager?
- Was sind die Vor- und Nachteile von Passwort-Managern?



Mögliche Anlaufstellen für eure Recherchen

- <https://de.wikipedia.org/wiki/Kennwortverwaltung>, eingesehen am 22.11.2015
- <http://keepass.info>, eingesehen am 22.11.2015
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, eingesehen am 22.11.2015
- <https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html>, eingesehen am 22.11.2015
- <http://www.stern.de/tv/10-tipps-so-erstellen-sie-sichere-passwoerter-3136120.html>, eingesehen am 22.11.2015

Tipps für eure Präsentation

- Gestaltet einen kleinen Flyer, der die wichtigsten Aspekte eures Themas stichpunktartig und übersichtlich festhält.
- Zeigt die grundlegende Funktionsweise eines Passwort-Managers an einem konkreten Beispiel wie z. B. KeePass.

Quellen- und Literaturangaben

- <http://www.sicherespasswort.com>, eingesehen am 22.11.2015
- https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html, eingesehen am 22.11.2015
- <https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/Umgang/umgang.html>, eingesehen am 22.11.2015
- <http://www.stern.de/tv/10-tipps-so-erstellen-sie-sichere-passwoerter-3136120.html>, eingesehen am 22.11.2015
- <http://www.faz.net/aktuell/feuilleton/medien/liste-der-schlechtesten-passwoerter-2014-13382590.html>, eingesehen am 22.11.2015
- <https://de.wikipedia.org/wiki/W%C3%B6rterbuchangriff>, eingesehen am 22.11.2015
- <https://de.wikipedia.org/wiki/Kennwortverwaltung>, eingesehen am 22.11.2015
- <http://keepass.info>, eingesehen am 22.11.2015

Hinweise zum Unterricht

Anhand dieser Aufgabe erarbeiten die Schülerinnen und Schüler arbeitsteilig Inhalte aus dem Modul 1.8:

- Datensicherheit: Risiken (z. B. Trojaner), Sicherheitsregeln (z. B. sichere Passwörter), Maßnahmen (z. B. Backup, Virenschutz)

Neben dem Sammeln von Informationen zu den angegebenen Themen steht die Präsentation von Ergebnissen mit sinnvoll ausgewählten Darstellungsmöglichkeiten im Mittelpunkt.

Beispiele für Produkte und Lösungen der Schülerinnen und Schüler

Gruppe 1 – Möglicher Auszug aus einer Verbote-Liste



Passwörter

Fehler, die du
unbedingt vermeiden sollst



1. Verwende niemals real existierende Wörter und schon gar nicht die Namen von Freunden oder Verwandten!
2. Verwende nie das gleiche Passwort für mehrere Dienste!
3. Speichere deine Passwörter niemals unverschlüsselt!
4. Notiere deine Passwörter nie auf leicht zugängliche Notizzettel.
5. Gib deine Passwörter nie an andere weiter!
6. ...

Gruppe 2 – Möglicher Auszug aus einer Gebote-Liste



Checkliste für sichere Passwörter



- ✓ Verwende lange Passwörter bestehende aus großen und kleinen Buchstaben, Ziffern und Sonderzeichen!
- ✓ Verwende Eselsbrücken, die dir beim Merken von Passwörtern helfen, z. B.:
 - Ausgedachter Satz:
Ich gehe freitags gerne in die Schule und koche nachmittags dann Spaghetti
 - Passwort aus den Anfangsbuchstaben:
lgfgidSukndS
 - Weitere Veränderungen:
 - „i“ und „l“ wird zu „1“
 - „und“ wird zu „&“
 - „S“ wird zu „\$“
 - (End)Passwort: 1gfg1d\$&knd\$
- ✓ Halte deine Passwörter geheim!
- ✓ Speichere und verschlüssele deine Passwörter mit einem Passwort-Manager!
- ✓ Ändere deine Passwörter regelmäßig!
- ✓ ...

Gruppe 3 – Mögliche Vorstellung eines Passwort-Managers

Passwörter im Griff mit KeePass



http://keepass.info/screenshots/keepass_2x/main_big.png, Stand: 22.11.2015

- KeePass ist ein Programm zum sicheren Verwalten von Passwörtern.
- Das Programm ist kostenlos erhältlich unter <http://keepass.info>.
- Grundsätzliche Vorgehensweise:
 - Programm downloaden und installieren.
 - Beim ersten Start neue Passwortdatenbank anlegen und mit einem Hauptpasswort verschlüsseln. Jedes mal, wenn man die Datenbank nun öffnen will, muss man das Hauptpasswort eingeben.
 - Neue Passwörter in der Datenbank anlegen oder bestehende Passwörter einsehen.
- Vorteil: Man muss sich nur noch das Hauptpasswort merken.
- Nachteil: Was, wenn man das Hauptpasswort vergisst oder die Passwortdatenbank kaputt geht?
- ...



Anregung zum weiteren Lernen

Das Bundesamt für Sicherheit in der Informationstechnik hält im Zusammenhang mit der Nutzung digitaler Medien zahlreiche interessante Artikel bereit, z. B.:

- Verschlüsselung von Daten und Kommunikation
https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/Verschluesselung_node.html
eingesehen am 22.11.2015
- Sicherheit beim Chatten
https://www.bsi-fuer-buerger.de/BSIFB/DE/DigitaleGesellschaft/KommunikationUeberInternet/ChatAberSicher/chat_apersicher_node.html
eingesehen am 22.11.2015
- Identitätsdiebstahl – Schutzmaßnahmen und Hilfe
https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/ID-Diebstahl/id-diebstahl_node.html
eingesehen am 22.11.2015